DUMPSARENA

Fortinet NSE 8 Written Exam

Fortinet NSE8_811

Version Demo

Total Demo Questions: 10

Total Premium Questions: 60

Buy Premium PDF

https://dumpsarena.com

sales@dumpsarena.com

QUESTION NO: 1

A company has just rolled out new remote sites and now you need to deploy a single firewall policy to all of these sites to allow Internet access using FortiManager. For this particular firewall policy, the source address object is called LAN, but its value will change according to the site the policy is being installed.

Which statement about creating the object LAN is correct?

A. Create a new object called LAN and enable per-device mapping.

B. Create a new object called LAN and promote it to the global database.

C. Create a new object called LAN and use it as a variable on a TCL script.

D. Create a new object called LAN and set meta-fields per remote site.

ANSWER: A

QUESTION NO: 2

A customer has a SCADA environmental control device that is triggering a false-positive IPS alert whenever the Web GUI of the device is accessed. You cannot create a functional custom IPS filter to exempt this behavior, and it appears that the device is so old that it does not have HTTPS support. You need to prevent the false positive IPS alerts from occurring. In this scenario, which two actions will accomplish this task? (Choose two.)

A. Create a URL filter with the Exempt action for that device IP address.

B. Change the relevant firewall policies to use SSL certificate-inspection instead of SSL deep-inspection.

C. Create a very specific firewall policy for that device IP address which does not perform IPS scanning.

D. Reconfigure the FortiGate to operate in proxy-based inspection mode instead of flow-based.

ANSWER: A C

QUESTION NO: 3

An administrator reports continuous high CPU utilization on a FortiGate device due to the IPS engine. Consider the global IPS configuration shown below.

```
config ips settings
 set packet-log-history 10
 set packet-log-post-attack 10
end
config ips global
 set fail-open enable
 set intelligent-mode disable
 set engine-count 0
end
```

Which two configuration actions will reduce the CPU usage? (Choose two.)

A. Reduce the number of packets being logged.

B. Increase engine-count to 2.

C. Enable intelligent mode.

D. Disable fail open.

ANSWER: A C

QUESTION NO: 4

Consider the following FortiGate configuration:

```
config firewall ssl-ssh-profile
   edit "custom-deep-inspection"
      config https
         set untrusted-cert {option}
      end
   next
end
```

Which command-line option for deep inspection SSL would have the FortiGate re-sign all untrusted self-signed certificates with the trusted Fortinet_CA_SSL certificate?

A. block

B. inspect

C. allow

D. ignore

ANSWER: D

QUESTION NO: 5

Refer to the exhibit.

```
config system interface
   edit "port1"
      set ip 10.10.10.3 255.255.255.0
   next
end

config firewall ippool
   edit "secondary_ip"
      set startip 172.16.1.254
      set endip 172.16.1.254
   next
end

config firewall central-snat-map
   edit 1
      set orig-addr "internal"
      set srcintf "port2"
      set dst-addr "all"
      set dstintf "port1"
      set nat-ippool "secondary_ip"
      set protocol 6
   next
end
```

Central NAT was configured on a FortiGate firewall. A sniffer shows ICMP packets out to a host on the Internet egresses with the port1 IP address instead of the virtual IP (VIP) that was configured Referring to the exhibit, which configuration change will ensure that ICMP traffic is also translated?

A.
```
config firewall central-snat-map
    edit 1
        set protocol 1
    next
end
```

B.
```
config firewall central-snat-map
    edit 1
        unset protocol
    next
end
```

C.
```
config firewall ippool
    edit "secondary_ip"
        set arp-intf 'port1'
    next
end
```

D.
```
config firewall central-snat-map
    edit 1
        set orig-addr "all"
    next
end
```

A. Option A

B. Option B

C. Option C

D. Option D

ANSWER: B

QUESTION NO: 6

A company has just deployed a new FortiMail in gateway mode. The administrator is asked to strengthen e-mail protection by applying the policies shown below.

• E-mails can only be accepted if a valid e-mail account exists.

• Only authenticated users can send e-mails out.

Which two actions will satisfy the requirements? (Choose two.)

A. Configure recipient address verification.

B. Configure inbound recipient policies.

C. Configure outbound recipient policies.

D. Configure access control rules.

ANSWER: A D

QUESTION NO: 7

You want to access the JSON API on FortiManager to retrieve information on an object.

In this scenario, which two methods will satisfy the requirement? (Choose two.)

A. Download the WSDL file from FortiManager administration GUI.

B. Make a call with the curl utility on your workstation.

C. Make a call with the SoapUI API tool on your workstation.

D. Make a call with the Web browser on your workstation.

ANSWER: A C

QUESTION NO: 8

You are asked to add a FortiDDoS to the network to combat detected slow connection attacks such as Slowloris.

Which prevention mode on FortiDDoS will protect you against this specific type of attack?

A. asymmetric mode

B. aggressive aging mode

C. rate limiting mode

D. blocking mode

ANSWER: B

QUESTION NO: 9

Refer to the exhibit.

```
ike 0:Dial-Up_0:30:Dial-Up:5: IPsec SA selectors #src=1 #dst=1
ike 0:Dial-Up_0:30:Dial-Up:5: src 0 7 0:0.0.0.0-255.255.255.255:0
ike 0:Dial-Up_0:30:Dial-Up:5: dst 0 7 0:10.10.10.0-10.10.10.255:0
ike 0:Dial-Up_0:30:Dial-Up:5: add dynamic IPsec SA selectors
ike 0:Dial-Up_1:2: moving route 10.10.10.0/255.255.255.0 oif Dial-Up_1(23) metric 15 priority 0 to 0:DialUp_0:5
ike 0:Dial-Up_1:2: del route 10.10.10.0/255.255.255.0 oif Dial-Up_1(23) metric 15 priority 0
ike 0:Dial-Up_1: deleting
ike 0:Dial-Up_1: flushing
ike 0:Dial-Up_1: deleting IPsec SA with SPI fa6915c1
ike 0:Dial-Up_1:Dial-Up: deleted IPsec SA with SPI fa6915c1, SA count: 0
ike 0:Dial-Up_1: sending SNMP tunnel DOWN trap for Dial-Up
ike 0:Dial-Up_1:Dial-Up: delete
```

A FortiGate is configured for a dial-up IPsec VPN to allow multiple remote FortiGate devices to connect to it. However, FortiGate A and B have problems connecting to the VPN. Only one of them can be connected at a time. If site B tries to connect while site A is connected, site A is disconnected. The IKE real-time debug shows the output in the exhibit when site A is disconnected.

Referring to the exhibit, which configuration setting should be executed in the dial-up configuration to allow both VPNs to be connected at the same time?

A. set route-overlap allow

B. set single-source disable

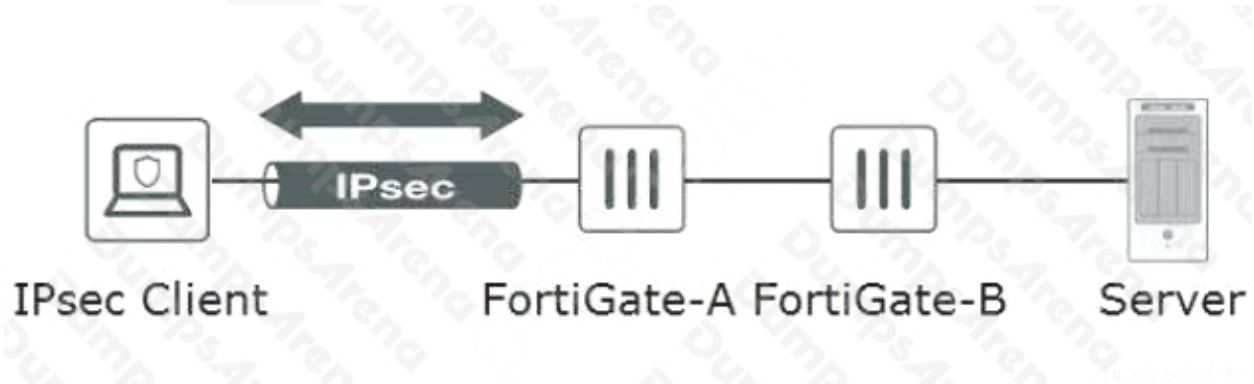
C. set enforce-unique-id disable

D. set add-route enable

ANSWER: A

QUESTION NO: 10

Refer to the exhibit.



Only users authenticated in FortiGate-B can reach the server. A customer wants to deploy a single sign-on solution for IPsec VPN users. Once a user is connected and authenticated to the VPN in FortiGate-A, the user does not need to authenticate again in FortiGate-B to reach the server. Referring to the exhibit, which two actions satisfy this requirement? (Choose two.)

A. Use Kerberos authentication.

B. Use the Collector Agent.

C. Use FortiAuthenticator.

D. FortiGate-A must generate a RADIUS accounting packet.

ANSWER: C D